Pilot program evaluating personal tablet device use across campus

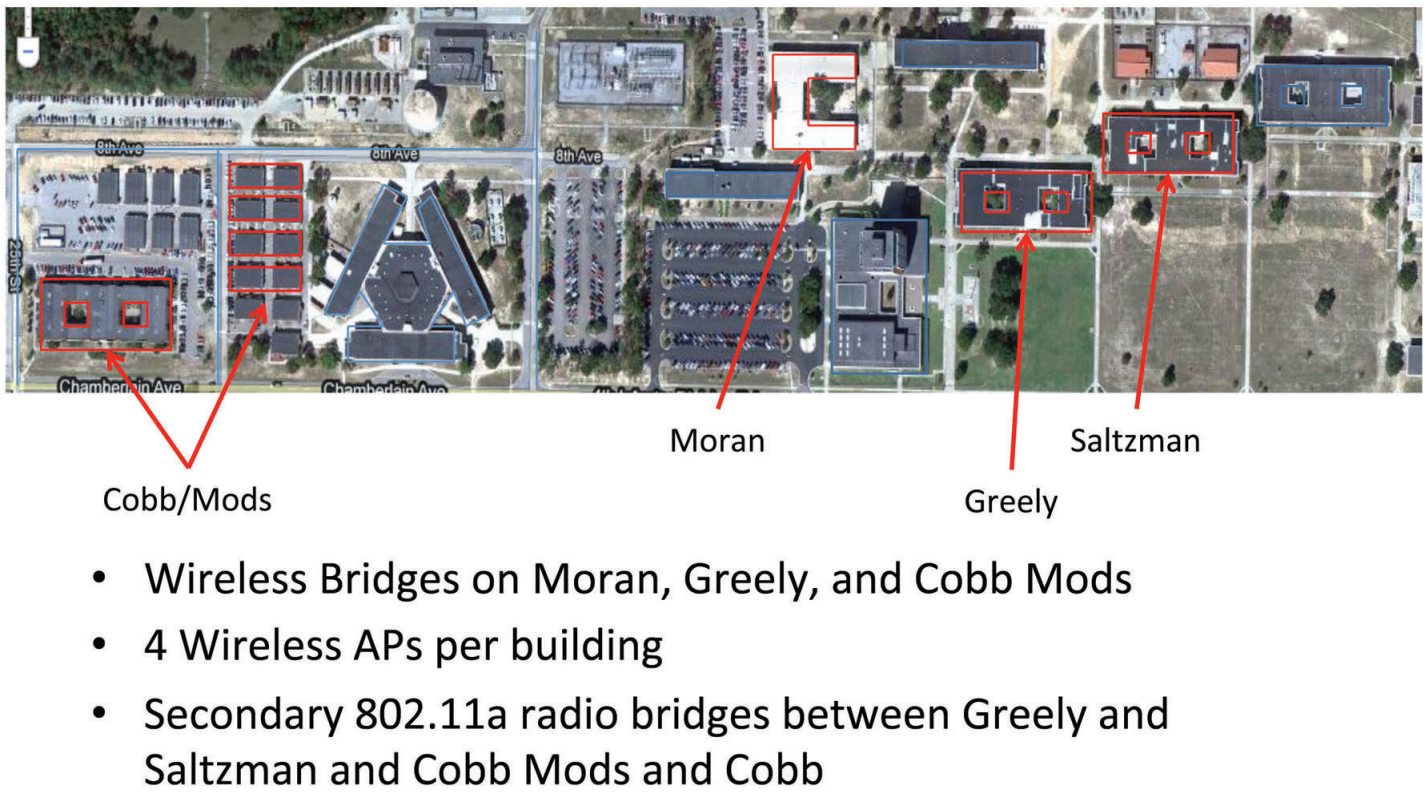
By LTC Gregory Motes and CPT Chris Braunstein

After the introduction of Apple's iPad in 2010, there was natural interest among leaders of the Army's education system to evaluate the potential of tablets running Smartphone operating systems for training support in military classrooms. With Soldiers' ongoing development of mobile applications at Fort Gordon, MG Alan R. Lynn, commanding general and Mr. Joe Capps, then deputy to the commanding general of the Signal Center of Excellence, worked in collaboration with MG Mark Bowman from the Army CIO/G6 to acquire 150 tablet devices for the SIGCoE's mobile computing pilot program. An additional 150 tablets were acquired for the parallel pilot program at the U. S. Military Academy. Both programs were given the restriction that the devices would not connect to the Non-secure Internet Protocol Router Network.

The prevalent belief at the time was that the inclusion of tablets with access to relevant information deemed useful for the students could increase performance in the classroom. With this, the SIGCoE formally created a pilot program called the SIGCoE Connected Personal Tablet pilot, which determined several areas useful for exploration, identifying three separate focus areas: academic administration, student socialization, and institutional learning.

Academic administration goals included determining how to use connected personal tablets for the students to send and receive information about pending or recent events, while providing a gateway of communication between the students and their class leaders, small group leaders, instructors and course adminis

(Continued on page 18)



This graphic shows the U. S. Army Signal Center of Excellence Connected Personal Tablet network layout on the Fort Gordon academic footprint.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Pilot program evaluating personal tablet device use across campus	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Signal Center of Excellence and Fort Gordon,Army Communicator,Signal Towers (Building 29808), Room 713,Fort Gordon,GA,30905-5301**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**7**	

(Continued from page 17)

trators. An example of this included using a calendar program on the device to allow administrators and leaders to note upcoming events and locations/ uniforms that the students need to be aware of, and to allowing instant access to a flowing schedule. There was also interest in connecting the students to Blackboard for ubiquitous access to classroom resources already provided to the students.

Student socialization goals included using the devices to connect the students to each other and to the larger community using social networking tools and norms. Among these are connections to MilBook and MilWiki, as well as social networking sites like FaceBook and Twitter. During the pilot program, multiple resources that the students could access switched from AKO username / password authentication to using CAC/PKI for authentication, which lessened the usefulness of the tablets and highlighted a significant challenge to mass adoption of new devices given the legitimate security concerns provided by untested and unintegrated devices.

Learning goals included examining course content that can be used for preparation, augmentation, replacement, refreshing and assessment. Preparation material includes any read-ahead material or courseware that instructors might require as a prerequisite to instruction. Currently a vast amount of content resides within Blackboard, and the SCPT intended to examine the ease and utility of converting that to a means that is acceptable on a tablet. Augmentation includes having material and tools that students can use as part of their normal coursework to increase their time to acquire the learning objectives. As an example, having an app that can be used to augment instruction on subnetting could be useful to students attempting to learn the complexities of that subject. Additionally, having the ability to use a tablet to port into a Cisco Switch, or to connect remotely to a server for management, can augment the instruction. Replacement is simply looking at courses and instruction that can be suited for distributed learning on a tablet allowing students to learn those topics without having to come to class.

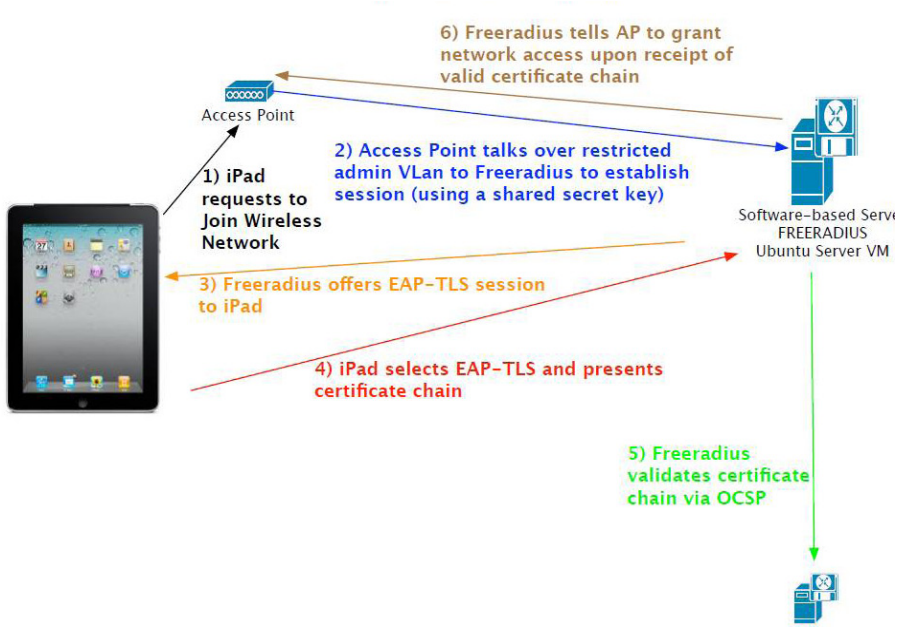
As the Army moves toward the goals of the Army Learning Model 2015, identifying courses and material that can be supplanted by digital device instruction is an area requiring exploration. Refreshing material is designed for alumni of a particular course to go back and review information from their studies to inform them in certain aspects of a problem. An example of that within the SIGCoE's context could be the eventual creation of course material from our Basic Officer Leadership Course and then to make that material available to students coming to SCCC as a refresher. Furthermore, as an increasing amount of content is available on personal devices, once a student graduates from a course, they should have alumni access to that information if they need to recall it during their current duty assignment.

The fifth dimension here is supported using tablets and apps to assess "Assessing Students." In addition to formal assessment, computer based training modules already in existence have shown numerous ways to provide checks on learning and self-assessment. With the data that can be collected across a wide range of apps, a depth of assessment tools and techniques can be applied to understand the student's learning styles and adapt the material based on their preferences. As an example, some students find videos favorable to detailed text, while others prefer to read the technical details in depth in order to grasp complex subjects.

Apps

One identified challenge with many of the pilot programs that are examining mobile devices is their lack of specific applications that can be provided to the early adopters. With the SCPT, students were provided with access to several commercial applications that could be used for classroom and office productivity, including applications to create new documents, spreadsheets and presentations, as well as apps that can assist in managing notes. Furthermore, they were encouraged to download additional free apps to provide feedback on the capabilities of those apps in relationship to professional military education. The users were informed that information they stored on the device not violate military regulations in terms of storing Personally Identifiable Information and meeting Data at Rest requirements. Furthermore, they were cautioned against creating or accessing information that was deemed For Official Use Only due to security concerns and the lack of a current Security Technical Implementation Guideline for the tablet.

Additionally, previous apps created by the SIGCoE were installed, including apps for Physical Readiness Training and Army Values. The SIGCoE also discussed the creation of a number of additional apps, including a Decision Matrix app, QR Code trainer, Signal Connect, and an app for Generator Power Distribution. Furthermore, the use of virtualized desktops that the tablets could access through VMware's View technology was presented as an option to allow the students to connect to complex Windows based applications like the unclassified training version of the Command Post of the Future or Network Monitor programs like SolarWinds.



Here is an illustration of the network authentication signal flow that occurs when joining the network.

Technology Management

Moving toward mixing public and custom apps created some interesting management problems addressed in the SCPT. On any of the current mobile operating systems, downloading apps from a public market required that the device use unique login accounts. Inclusion of the iPad as one of the tablets tested also meant that we had to individually activate the device through iTunes and manually load the apps to the devices.

As discussed below, the technology for "imaging" devices matured during the course of our 15 month pilot. This eased some of the technology management hurdles for iOS devices. At the beginning of the effort, though, individual iTunes accounts were created for each of the students and tied to a domain email address provided by the SIGCoE. This allowed the legal transfer of applications purchased for "Student 1" to stay with the tablet as it was reassigned to future classes. Subsequently, bulk purchasing of applications has also made it easier for a school to volume license applications for legal inclusion onto school owned devices.

A further goal of the SCPT was to examine the procedures and technical infrastructure required to support the program. Configuration management was a big challenge because many management tools were in their infancy or did not exist. Early on we had to wipe, update, and prepare each individual tablet one at a time in an assembly line type operation. This was further complicated by the fact that the tablets required a USB connection to a computer in order to activate prior to use. We initially had a bank of laptops with iTunes installed that students would use during the initial issue process. A new operating system update fixed this problem and students were able to complete the tablet setup process without connecting to a computer.

Our final issue process was to issue the tablets and accessories, require students to read and to sign the Acceptable Use Policy and hand receipt, to connect their tablets to a "bootstrap" network that would only allow them to connect to a web server to download a configuration profile, and to finally download an application to complete a survey and proficiency test. This process initially took two hours per group of 20 students, and was eventually reduced to approximately 45 minutes depending on how many questions students had.

Even though we came up with a pretty manageable process for issue and turn-in of tablets, we were still faced with additional problems. It was cumbersome to keep whatever tablets we had in our inventory updated to the latest operating system due to having to plug each one into a computer for updates.

We were also concerned about students' personal information persisting between updates, requiring a manual inspection of each tablet to ensure that students were wiping them as instructed during turn-in. Keeping a class worth of tablets charged for the next issue required multiple power strips and power outlets.

Eventually we acquired a cart with storage shelves for 30 tablets with 30-pin dock connectors for each device that solved all of these issues. The cart was mobile and had a standard power cord that would keep the tablets charged while in storage. A single USB cable connected to a computer allowing for the wiping, updating, and configuration of all 30 tablets in the cart. An application called "Configurator" allowed us to wipe all the tablets, update them to the latest operating system, and push apps (both enterprise and from the iTunes store) and configuration settings to each device simultaneously.

Many of the goals of the SCPT required Internet functionality. There was value in examining the effects and management challenges of mobile devices on a Local Area Network.

Leaders at the SIGCoE quickly determined that a 100% com

(Continued on page 20)

(Continued from page 19)

mercial network would be. required and set out to build a cheap and reliable testing ground for the students, acquiring a standard commercial cable internet connection that provided 25 Mbps down / 3 Mbps up of bandwidth. We constructed a wireless repeater network using 802.11g access points and bridges.

The bridges were installed on the top of buildings and the access points were wired using CAT 5e cable. All of the equipment was powered using Power over Ethernet switches. Since we only were supporting 150 devices and a relatively small footprint we decided to keep everything in the same private subnet, allowing us to keep the wireless equipment in the Data Link layer (Layer 2) of the Open Systems Interconnect model. Because of this we did not have to install routers in each building that vastly reduced the cost and management requirements of the network. Despite this being an "open" Internet connection, we still were required to maintain as much adherence to Army Information Assurance Regulations as possible (AR 25-1 and 25-2). We installed a firewall at the perimeter of the network that blocked all non-web services.

Initially we were concerned that this would cause problems with applications that the students were downloading, but we discovered that almost all apps use web ports and protocols for data transfer. This could be a general trend, or just a reflection of our small user base. A transparent open source web proxy was also installed to block access to restricted material (pornography, gambling, hacking, etc.) and for auditing purposes. All web traffic was redirected from the edge router to the web proxy server using the Web Cache Communication Protocol. The redirected web traffic was also cached locally in an attempt to reduce bandwidth usage of the Internet connection.

A method was needed to ensure that only SIGCoE issued tablets were authorized to connect to our commercial wireless network. This would ensure that only authorized students were connecting as well as reducing the bandwidth needs and monitoring requirements. There are currently no known viruses/malware on the iOS platform (other than on jailbroken devices - which was not possible for the iPad 2 with the version of the operating system that we were using). By limiting the network to only SIGCoE issued tablets we could greatly reduce the risk of a virus or other rogue element causing data leakage or other destructive behaviors on the network. Most non-enterprise wireless networks use a pre-shared key for access control or are open access. Using a pre-shared key would have been problematic for us. We would not be able to ensure that students didn't share the password with other individuals and would have to constantly monitor the network for rogue devices. After a class turned in their equipment we would have to cycle the key on every access point, which would have been time consuming and pointless. We needed to use an enterprise class authentication system that was not based on credentials. Based on this fact we designed a certificate based authentication system that ensured only SIGCoE issued iPads that were signed out to a student would be authorized on the network.

The SIGCoE had already built a virtualization cluster for hosting code repositories and other development tools, so we had plenty of server space for this solution. The first step was to stand up a Remote Authentication Dial In User Service server. RADIUS is a client/server protocol that can be used to authenticate users or devices before granting them access to a network. This server would act as the "gatekeeper" to our network, only allowing devices with valid certificates onto the network. When a device attempts to connect to a wireless access point a connection is established between the access point and the RADIUS server over an administrative Virtual Local Area Network to establish a session using a shared secret key.

Next, the RADIUS server offers an Extensible Authentication Protocol - Transport Layer Security session which is established between the tablet and the RADIUS server. This session is unique because the tablet is not assigned an Internet Protocol address at this point ensuring that it can only communicate with the RADIUS server and not other devices on the network or the internet. The tablet presents the digital certificate chain to the RADIUS server over the encrypted tunnel. Finally, the RADIUS server uses the Online Certificate Status Protocol to validate the certificate chain and either approves or disapproves network access.

We also needed a way to generate the digital certificates in an automated process that could also be controlled by the SIGCoE during the tablet issue process. We created a Simple Certificate Enrollment Protocol server that could issue and revoke digital certificates. The iOS operating system includes support for SCEP, OCSP, RADIUS, and EAP-TLS. Additionally, all of these protocols can be configured using a "configuration profile" which is an Extensible Markup Language file that allows for the distribution of configuration information to iOS devices. These profiles can be installed on a device over a USB connection, by sending it to a device via e-mail or a website hyperlink, or through a Mobile Device Management solution that would push profiles to devices over the air. We generated a configuration profile for each class issue which included the SCEP enrollment request, the Wi-Fi network SSID settings, and two self-signed digital certificates to ensure the validity of the servers that the tablets would authenticate with to

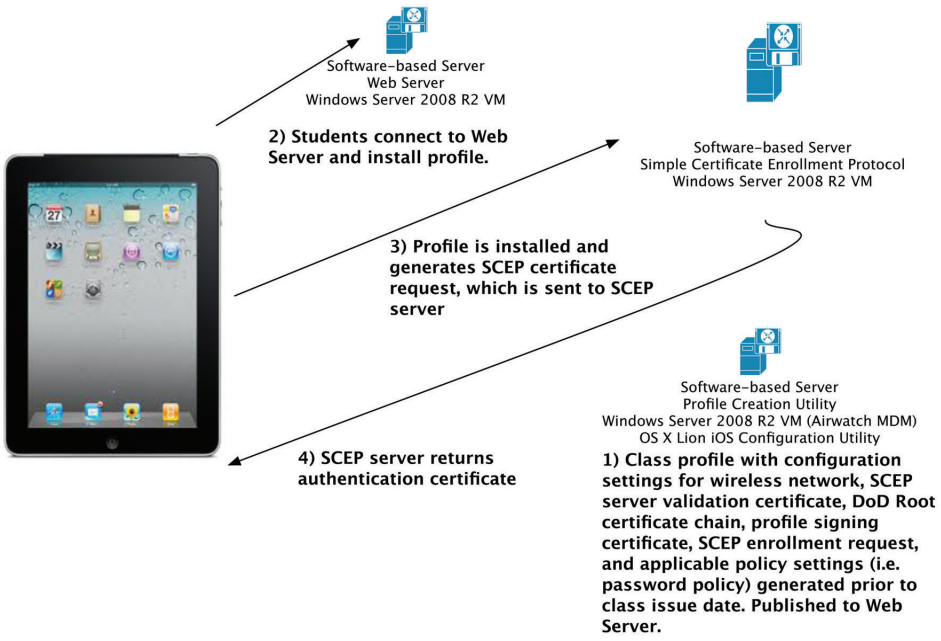
protect against man-in-the-middle-attacks. This configuration profile was also digitally signed to protect against tampering with the profile and so that tablets could verify its authenticity.

This system had additional control measures built-in. We would only allow the SCEP server to issue certificates during the issue process, which ensured that rogue tablets could not get a certificate during non-issue times.

The SCEP certificate issue process and configuration profile download were restricted to the "bootstrap" network that only connected to the web server hosting the configuration profile, ensuring that tablets would only be able to be provisioned during controlled issue. We could disable the "bootstrap" network when it was not in use, ensuring that attackers would not be able to maliciously attempt to get the configuration profile or digital certificate chain.

A configuration profile could not be extracted from an iOS tablet, ensuring that users could not transfer their certificates to another device. A user could remove the configuration profile by connecting the device to a laptop via USB and restoring the operating system, but this would permanently remove the profile which would mean that their device would not be allowed onto the network. A configuration profile could also configure further restrictions such as stopping the camera from working or removing access to the iTunes market - almost all of the iOS configuration settings and features could be controlled. Using this method we could tie network access to our Acceptable Use Policy, ensuring that devices conformed to our policy before being allowed to connect to the network. We could also revoke the certificate on the SCEP server for a particular device, allowing us to remove individual devices from the network.

This system would also work on Android based devices, however extra care would have to be taken due to the fact that the Android operating system does not use a "configuration profile" system for device management.



Initial provisioning process for an iPad with certificate authentication.

The digital certificate could be stored in an encrypted form using a Public Key Infrastructure token such as a Common Access Card on the device SD Card or internal storage. CAC card readers are available for purchase today, although they are expensive and the software has not matured enough for exclusive day to day use.

We performed a limited amount of testing of Android tablets but never implemented an Android compatible version of this solution.

In addition to the servers required for the network authentication system, we used an open source network monitoring solution called Zenoss. We installed Zenoss as a virtualized application that was managed from a web console. Using Zenoss we could monitor all aspects of the network through polling (pinging devices on the network to check their status) as well as through the Simple Network Management Protocol.

SNMP exposes management data in the form of variables on the managed systems, which describe system configuration and state. A managed device runs an "agent" that can send asynchronous notifications called "traps" to the management platform containing data such as CPU usage, temperatures, bandwidth utilization, etc. An agent can also be polled through a "GetRequest" that will return the status of desired variables. All variables are defined by management information bases which describe the nature of a device subsystem.

Overall, the tablets presented a moderate management load to the network. Traditional network monitoring must still be performed (link status, service availability, etc). We had reduced the concern for malware and viruses significantly, but still had to maintain active monitoring of the servers. An intrusion detection system would have increased the likelihood of detecting an attack on the network, although we did not install one

(Continued on page 22)

(Continued from page 21)

because we did not have the necessary manpower to fine tune and monitor it. An average of one or two tablets were broken per class during the course of the pilot. Technical support requests were much lower than if using desktop or laptop based systems, averaging less than one support request per class. Additional challenges arose such as wireless access point coverage, bridge link alignment, and ISP outages that added to the management tasks.

Classes

During the initial planning for the SCPT, we discussed issuing devices to multiple different courses at the Signal Center, including the Signal Captains' Career Course, the Functional Area 53 Information Systems Manager Qualification Course, as well as consideration for the Warrant Officer classes.

Ultimately, it was decided that the best effort was to focus on a single course and try to establish continuity over time with the instructors, small group leaders and training developers. Of the groups invited to the initial planning meetings, the SCCC course leaders were the most enthusiastic about participating in the SCPT, so the decision was made to issue them the devices.

Each SCCC has 40 students and 2 small group leaders assigned, so 42 devices were set aside for each of 3 courses, with remaining devices available to the application developers and a limited number of instructors and cadre.

Data Collection Metrics

Early on, it was predicted that success for this pilot hinged on the willingness of the cadre to explore the utility of the devices, as well as ensuring that the technology did not disrupt the course programmed instruction. Additionally, it was determined that the inclusion of the Army Research Institute for Behavioral and Social Science could provide a resource for analyzing whether or not the devices were actually beneficial to users, as opposed to other programs which largely rely on anecdotal evidence of improvement.

At the time of this publication, ARI is compiling the results of surveys presented to students when they were issued the devices and comparing them to surveys presented at the completion of the course.

Key Challenges and Lessons

Upon approval for the program, several key tasks and milestones were established, each meeting varied levels of challenge. Since the approval and purchase of the devices originated at Army CIO/G6 and the Army G8 level, it took less than 3 weeks to receive the 150 devices. At the time, three other areas still needed to be in place to bring the program up to the desired operation level, including the implementation of a commercial wireless network, the legal approval of an Apple Enterprise license for custom app distribution and the mobile device management solution.

Using on-hand wireless access points and connecting to an existing server stack used for code repository was easily accomplished with collaboration between the SIGCoE programmers and cadre at the Cyber Leader College in the 442nd Signal Battalion. The internal WiFi was not yet connected to a commercial network due to a local issue with the Internet Service Provider that connected the public Internet to Fort Gordon. In short, the company that provided those services had just been acquired by a different company and could not take on new clients until after the acquisition had been finalized. This left the SCPT in a time delay that lasted several months.

In the meantime, instead of leaving the tablets in wall lockers awaiting a public connection, we decided to issue the devices to the first class with the caveat that they would not be connected to the Internet during their class.

This allowed the SCPT to gather some control group statistics to answer the question, "Will the tablets, without connectivity, provide positive outcomes in the classroom?" As predicted, the students embraced the idea of having tablets as part of their course equipment, but without a connection found them to be extremely limited. Some used them to take notes and read PDFs that they could download from other Internet connections (home, hotel, coffee shop, etc), but found that the lack of connectivity in their classrooms did not encourage them to use the devices to the extent of their potential.

By the end of the first class, we had solved our ISP issues and deployed the local WiFi that allowed students to connect to the Internet. We still awaited approval of an Enterprise license to distribute custom apps experiencing three separate challenges. The first challenge was to get the Fort Gordon legal counsel to review the Enterprise developer agreement and determine who at the Signal Center could be authorized to bind the Center to the agreement. In this matter, we had considerable assistance from Apple's federal accounts managers for clarification on the terms and conditions, ultimately determining that a contractor officer Representative appointed by the contracting officer could sign the agreement. The second issue was that Apple requires a Data Universal Numbering System Number, which was something we didn't have specifically assigned to our unit. After some research, we were able to find a DUNS that we could put that would satisfy Apple's requirements. The final issue was simply paying the $299 for the fee. As a startup organization, we have

found that working through the processes to spend money is a very time consuming task for both small and large purchases.

Another challenge was adoption and acceptance within the schoolhouse. Although the SCCC leadership was enthusiastic and supportive of the SCPT, we were overly cautious about forcing the instructors, students and small group leaders into inserting too many components of the program into their classes and administrative features.

The result was that some areas that we thought should have been tested were not incorporated into the class. As an example, each student was given a wireless keyboard to assist with typing using the touch screen. One question we thought would be interesting to ask in a pretest was to determine students' thoughts about typing a 1000 word written assignment while using a tablet, then to ask them the same question at the end of the course. The hypothesis was that once a student used a wireless keyboard, trepidation about typing on the mobile device form factor would diminish. We suggested that the SCCC faculty require their students turn in one of their written assignments after writing the paper on the tablet. When we retrieved the first group of iPads, we were disappointed to find that many of the keyboards remained unopened and unused.

Despite this, the reaction to the inclusion of mobile tablets into the classroom was generally well received. In post class discussions, many of the students could clearly see the potential for mobile computing in a training environment and were eager to offer ideas of how the devices could be used in further classes. They were very interested in the ability to use tools that can assist them during their practical exercises, with access to the desktop and server applications at the top of their request list.

As the pilot is nearing its conclusion, we eagerly wait for the results from ARI to find the areas that were most positive in order to make a proposal for future efforts. While more work is required from security and policy perspectives, tt is clear from our observations that the inclusion of personal mobile computing in the military is in the future.

LTC Gregory Motes ***was the chief of the U.S. Army's Mobile Applications Branch at Fort Gordon, Ga, creating the concept for the SCPT program. LTC Motes spoke about mobile apps at several conferences or forums in the past 18 months and is one of the most influential people in Army mobility.***

CPT Chris Braunstein ***previously served as the lead engineer and automation management officer for the U.S. Army's Mobile Applications Branch at Fort Gordon. CPT Braunstein created a secure server infrastructure to allow connectivity between students and the Internet and has personally written 42 apps for iPhone or Android.***

Acronym QuickScan

AKO – Army Knowledge Online
AR – Army Regulation
ARI – Army Research Institute
AUP – Acceptable Use Policy
CAC – Common Access Card
CIO – Chief Information Officer
CPU – Central Processing Unit
DAR – Data at Rest
DECMAT – Decision Matrix
DUNS – Data Universal Numbering System
EAP-TLS – Extensible Authentication Protocol - Transport Layer Security
FOUO – For Official Use Only
iOS – iPhone Operating System
IP – Internet Protocol
ISM – Information Systems Management
ISP – Internet Service Provider
LAN – Local Area Network
Mbps – Mega Bits Per Second
MDM – Mobile Device Management
NIPRNET – Nonsecure Internet Protocol Router Network
OCSP – Online Certificate Status Protocol
OSI – Open Systems Interconnection
PII – Personally Identifiable Information
PKI – Public Key Infrastructure
PoE – Power over Ethernet
QR – Quick Response
RADIUS – Remote Authentication Dial In User Service
SCCC – Signal Captains Career Course
SCEP – Simple Certificate Enrollment Protocol
SCPT – SIGCoE Connected Personal Tablet
SIGCoE – Signal Center of Excellence
SNMP – Simple Network Management Protocol
SSID – Service Set Identifier
STIG – Security Technical Implementation Guide
USB – Universal Serial Bus
VLAN – Virtual Local Area Network
XML – Extensible Markup Language